

## Juniper Networks

### NetScreen Release Notes

Product: NetScreen-Security Manager 2004 FP3-IDPr1

Version: FCS

Release Status: Public

Part Number: 093-1525-000, Rev. B

Date: 6-16-05

## Contents

1. ["Version Summary" on page 2](#)
2. ["New Features" on page 2](#)
3. ["Changes to Default Behavior" on page 3](#)
4. ["Addressed Issues" on page 3](#)
5. ["Known Issues" on page 3](#)
  - [Section 5.1 "Limitations of Features"](#)
  - [Section 5.2 "Compatibility Issues"](#)
  - [Section 5.3 "Known Issues"](#)
  - [Section 5.4 "Known Issues in ScreenOS 5.0 That Affect NetScreen-Security Manager 2004 FP3-IDPr1"](#)
6. ["Getting Help" on page 7](#)

## 1. Version Summary

This version of Juniper Networks NetScreen-Security Manager 2004 Feature Pack 3 (FP3) supports IDP functionality for the Juniper Networks' ISG 2000 with ScreenOS 5.0.0-IDP1.

The ISG 2000 is a purpose-built, high-performance security system designed to provide a flexible solution to medium and large enterprise central sites and service providers. The ISG 2000 security system integrates firewall, VPN, traffic management and Intrusion Detection and Prevention (IDP) functionality in a low-profile, modular chassis.

The ISG 2000 is built around Juniper Networks fourth-generation purpose-built GigaScreen3 ASIC, which provides accelerated encryption algorithms. The ISG 2000 supports flexible I/O configuration with four- and eight-port 10/100 modules and two-port gigabit modules.

ScreenOS 5.0.0-IDP1 is the latest software version based on the ScreenOS 5.0.0 firmware branch for the ISG 2000 security system.

Note that you must install and use the appropriate version of NetScreen-Security Manager 2004 FP3-IDPr1 to configure and manage the ISG 2000 and the ISG 2000 security modules.

## 2. New Features

The following is a partial list of new features and enhancements in this release:

- **Integrated Intrusion Detection and Prevention (IDP) Mechanisms.** IDP extends Firewall/VPN functionality to protect the network against application level threats such as those proliferated by worms, Trojans, hackers, and spyware. The security modules for the ISG 2000 support multiple intrusion detection mechanisms including stateful signatures, protocol anomaly detection, and backdoor. IDP's traffic anomaly, SYN protector, and IP spoof are pre-existing ScreenOS features.
- **Support for all IDP Protocols And Contexts.** The security modules for the ISG 2000 provide extensive coverage of known and unknown threats by decoding 60+ protocols and searching within 500+ service fields, with pre-defined attack objects, as well as customizable ones.
- **Zone-based and Other Virtualization Features for IP Policies.** Use NetScreen-Security Manager to define intrusion detection and prevention policies not only by IP addresses but by zones, and to contain policies and enforcement. VLAN-tags, overlapping IP addresses in route mode are also supported.

- **VPN Aggression to Intrusion Prevention Services.** You can further extend policy- and route-based VPNs to IP policies enabling you to inspect de-tunneled traffic at the network and application level.
- **Role-based Administration for Firewall and IP Rulebases.** You also have the ability to separate and filter between FW/VPN and IP rulebases (tab navigation) as an option.

### 3. Changes to Default Behavior

None.

### 4. Addressed Issues

The following are addressed issues in this release of NetScreen-Security Manager 2004 FP3-IDPr1.

- **23048** – The destination address did not appear in the Log Viewer for FTP Reply Error: Nested Reply attacks.
- **22776** – Updating a device configuration froze at 85% completion.
- **22755** – Unassigning a policy from Vsys unloaded the IDP policy at the root level.
- **22394** – Custom reports did not display the correct number of logs.
- **21964** – The Log Viewer displayed the wrong rule number for IDP policies.
- **21404** – The UI did not save user preferences unless you logged out and logged back in.
- **20758** – Attack updates did not work when you were logged in under a subdomain.

### 5. Known Issues

This section describes known issues with the current release.

- [Section 5.1 “Limitations of Features”](#) identifies features that are not fully functional at the present time, and are not supported for this release.
- [Section 5.2 “Compatibility Issues”](#) describes known compatibility issues with other products, including but not limited to specific Juniper Networks’ appliances, versions of ScreenOS, Internet browsers, and other vendor devices. Whenever possible, information is provided for ways to avoid the issue, minimize its impact, or in some manner work around it.

- [Section 5.3 “Known Issues”](#) describes deviations from intended product behavior in NetScreen-Security Manager as identified by Juniper Test Technologies through their verification procedures. Again, whenever possible, information is provided to assist the customer in avoiding or otherwise working around the issue.
- [Section 5.4 “Known Issues in ScreenOS 5.0 That Affect NetScreen-Security Manager 2004 FP3-IDPr1”](#) describes deviations in ScreenOS 5.0r9 that affect this release of NetScreen-Security Manager as identified by Juniper Test Technologies through their verification procedures. Again, whenever possible, information is provided to assist the customer in avoiding or otherwise working around the issue.

## 5.1 Limitations of Features

The following limitations are present at the time of this release.

**Enterprise Security Profiler functionality is currently not available.** This functionality will be available in a later release. Other standalone-IDP features including Honeypot are planned to be made available later in 2005.

**Sniffer mode not supported.** The ISG 2000 is always deployed inline. You can not deploy the ISG 2000 with an external TAP or SPAN port on a switch. The Tap mode option is however, available supporting passive, inline detection of application layer threats. Sniffer mode for the TAP/SPAN port is currently available on standalone IDP devices only.

**IDP Manager does not support management of the ISG 2000 or the ISG 2000 security modules.** You must install NetScreen-Security Manager FP3-IDPr1 to manage the ISG 2000 and security modules.

## 5.2 Compatibility Issues

**Terminology differences in ScreenOS and Netscreen-Security Manager.** In IP Actions, the term “block” is used in DI and in the UI of IDP Manager. NetScreen-Security Manager however, uses the term “drop” for the same action.

## 5.3 Known Issues

The following are known deficiencies at the time of this release. Whenever possible, a work-around is suggested following the description of the problem. Workaround information starts with “W/A:”

- **23713** – After installing or upgrading the UI, occasionally many predefined attack groups will show empty members the first time you login to the UI.

W/A: Logout of the UI, and then re-login. When you view predefined attack groups, the members will appear.

- **23516** – You are limited in updating multiple Vsys at the same time if these Vsys belong to the same root device. The scenario includes multiple admins logging in at the same time, and attempting to update various Vsys in the same root device.
- **23382** – Installing the management system on Linux AS sometimes produces errors.

W/A: Run the system update utility to upgrade your system with the latest patches and packages. Then, run the installer script again.

- **23350/23586** – When upgrading firmware on the device, NetScreen-Security Manager is not able to retrieve the latest version of the detector.so.

W/A: After upgrading, you must re-import the device.

- **23222** – You are not able to assign interfaces in the same module to different aggregate interfaces with NS2000. You can assign all the interfaces in the same module to one aggregate interface only.
- **23150** – The policy for IP action logs appears as unknown in the Log Viewer.
- **23313** – The detector.so version is not displayed in virtual systems. You can only view the version in the root device.
- **22869** – If the signature package includes deleted attacks, blank logs for the attack appear in the Log Viewer, until you update the device.
- **22543** – When importing a device, Vsys devices are in a "exist on phy device" state. When you model the Vsys, the "exist on phy device" is not set. When you update the modeled device, you must modify the "exist on phy device" attribute in root to true.

W/A: Reimport the root device to update the vsys attributes.

- **22444** – Custom attacks do not appear in the log criteria.

## 5.4 Known Issues in ScreenOS 5.0 That Affect NetScreen-Security Manager 2004 FP3-IDPr1

The following are known issue in ScreenOS 5.0 that specifically affects this release of NetScreen-Security Manager:

- **48987** – Using NetScreen-Security Manager to upgrade security devices running ScreenOS 5.0.0 over a slow network connection (if the image download takes over 5 minutes), occasionally causes updates to time out.

W/A: In most cases, upgrading to ScreenOS 5.0.0 r10 resolves this issue. Refer to the table below for more information describing resolution of this issue in specific branches of ScreenOS.

- **45418/48460** – Devices are not able to save the key used to connect to the NetScreen-Security Manager Device Server. This causes the NSM agent on the security device to have to re-negotiate the key every time the security device restarts. The key re-negotiation process can take up to 15 seconds. One side effect of this issue is that when you restart the Device Server, this will also cause key renegotiation for all other security devices running it manages. This may cause system performance degradation that then affects the management of all security devices.

W/A: In most cases, upgrading to ScreenOS 5.0.0 r10 resolves this issue. Refer to the table below for more information describing resolution of this issue in specific branches of ScreenOS.

- **43001** – If you use NetScreen-Security Manager to upgrade the firmware on a device from ScreenOS 5.0.0 to ScreenOS 5.1, the security device crashes.

W/A: In most cases, upgrading to ScreenOS 5.0.0 r10 resolves this issue. Refer to the table below for more information describing resolution of this issue in specific branches of ScreenOS.

The table below describes specific releases of ScreenOS that resolve the issues referenced above, or provides other workaround information:

Issue	5.0.0	5.0.0 r9 for 5000 M2	5.0.0-GPRS.r8.5	5.0.0 WLAN	5.0.0 r9 for ISG 1000/ISG 2000	5.0.0IDP1
48987	5.0.0 r10	Upgrade the device firmware out-of-band using the CLI or WebUI.	Upgrade the device firmware out-of-band using the CLI or WebUI.	5.0.0 r10	5.0.0 r10	5.0.0IDP1 r2
45418/48460	5.0.0 r10	Upgrade the device firmware out-of-band using the CLI or WebUI.	Upgrade the device firmware out-of-band using the CLI or WebUI.	5.0.0 r10	5.0.0 r10	5.0.0IDP1 r2
43001	5.0.0 r10	5.2	5.2	5.0.0 r10	5.0.0 r10	5.0.0IDP1 r2

## 6. Getting Help

For more assistance with Juniper Networks products, visit:

[www.juniper.net/support](http://www.juniper.net/support)

Juniper Networks occasionally provides maintenance releases (updates and upgrades) for ScreenOS firmware. To have access to these releases, you must register your NetScreen device with Juniper Networks at the above web address.

Copyright © 2005 Juniper Networks, Inc. All rights reserved.

Juniper Networks, the Juniper Networks logo, NetScreen, NetScreen Technologies, the NetScreen logo, NetScreen-Global Pro, ScreenOS, and GigaScreen are registered trademarks of Juniper Networks, Inc. in the United States and other countries.

The following are trademarks of Juniper Networks, Inc.: Deep Inspection, ERX, ESP, Instant Virtual Extranet, Internet Processor, J-Protect, JUNOS, JUNOScope, JUNOScript, JUNOSe, M5, M7i, M10, M10i, M20, M40, M40e, M160, M320, M-series, MMD, NetScreen-5GT, NetScreen-5XP, NetScreen-5XT, NetScreen-25, NetScreen-50, NetScreen-100, NetScreen-204, NetScreen-208, NetScreen-500, NetScreen-5200, NetScreen-5400, NetScreen-IDP 10, NetScreen-IDP 100, NetScreen-IDP 500, NetScreen-IDP 1000, IDP 50, IDP 200, IDP 600, IDP 1100, ISG 1000, ISG 2000, NetScreen-Global Pro Express, NetScreen-Remote Security Client, NetScreen-Remote VPN Client, NetScreen-SA 1000 Series, NetScreen-SA 3000 Series, NetScreen-SA 5000 Series, NetScreen-SA Central Manager, NetScreen Secure Access, NetScreen-SM 3000, NetScreen-Security Manager, GigaScreen ASIC, GigaScreen-II ASIC, NMC-RX, SDX, Stateful Signature, T320, T640, and T-series. All other trademarks and registered trademarks are the property of their respective companies.

Information in this document is subject to change without notice.

No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without receiving written permission from:

Juniper Networks, Inc.  
ATTN: General Counsel  
1194 N. Mathilda Ave.  
Sunnyvale, CA 94089  
U.S.A.

[www.juniper.net](http://www.juniper.net)